IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Timothy M. Moore
Application No.: 09/694,514
Filed: October 23, 2000
Customer No.: 22971
Attorney Docket No.: 155608.02
Group Art Unit: 2132
Examiner: Kambiz Zand
Confirmation Number: 9639
Title: Security Link Management in Dynamic Networks

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

AMENDMENT AND RESPONSE TO NOTICE ON NON-COMPLIANT AMENDMENT (37 CFR 1.21) DATED MAY 31, 2006 AND OFFICE ACTION DATED NOVEMBER 25, 2005

Dear Sir,

Per the Notice of Non-Compliant Amendment (37 CFR 1.121) dated May 31, 2006 we have now made the appropriate corrections and have each amendment on a separate sheet.

Claims 1, 5, 16, 21 and 22 are amended.

Claims 10, 11, 20, 27 and 28 are canceled.

No claims are added.

Claims 1-9, 16-19, 21-26 and 33-36 remain pending.

Claim Listings begin on page **2** of this response.

Remarks begin on page **8** of this response.

THE CLAIMS

A detailed listing of pending claims 1-9, 16-19, 21-26 and 33-36 is provided below. A status identifier is provided for each claim in a parenthetical expression following each claim number.

1. (Currently Amended) A method of providing a mobile computing unit ~~machine~~ with privileged access to a computing resource, the method comprising the steps of:

determining that the mobile computing unit has failed to present adequate user identifying information when attempting to access the computing resource;

obtaining credentials with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit;

providing the credentials to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource; and

establishing limited access to the computing resource using authorization information obtained from the authenticator ~~to reflect~~ that reflects a relative security level ~~credentials~~ for a user of the mobile computing unit, the authorization information corresponding to the authenticated identity of the mobile computing unit.

2. (Original) The method of claim 1 wherein the mobile computing unit communicates with the computing resource using at least one wireless link.

3. (Original) The method of claim 1 wherein the authorization information includes a key for encrypting communications from the mobile computing unit to an input port.

4. (Original) The method of claim 3 wherein the key is a symmetric session key.

5. (Currently Amended) The method of claim 1 ~~further comprising, prior to the obtaining step, comprising~~ wherein the determining step further comprises detecting a failure of a user of the mobile computing unit to complete a logon to access the computing resource.

6. (Currently Amended) The method of claim 1 ~~further comprising, prior to the obtaining step,~~ wherein the determining step further comprises determining that the mobile computing unit does not have a certificate to prove machine identity.

7. (Original) The method of claim 1 further comprising the step of storing the unique machine identifier on the mobile computing unit for subsequent use.

8. (Original) The method of claim 1 further comprising the step of storing the certificate on the mobile computing unit.

9. (Original) The method of claim 1 further comprising the step of receiving the unique machine identifier.

10 – 15. (Canceled)

16. (Currently Amended) A method of providing a user secure access to a computing resource from an external site, the method comprising the steps of:

sending a request to access a computing resource;

providing a user identifier, the user identifier corresponding to an asserted identity, to a proxy authenticating server via a remote access point;

providing, in response to a challenge, ~~credentials~~ a certificate to authenticate the asserted identity, to the proxy authenticating server via the remote access point; and

receiving an address for sending and receiving data to and from the computing resource, the address corresponding to limited access to the computing resource based on the asserted identity.

17. (Original) The method of claim 16 wherein the address for sending and receiving data is a universal resource locator.

18. (Original) The method of claim 17 further comprising receiving by the user a key for encrypting communications to the computing resource.

19. (Original) The method of claim 18 further comprising using the key to decrypt communications from the computing resource.

20. (Canceled)

21. (Currently Amended) A computer-readable medium having computer executable instructions for performing the steps of a method of providing a mobile computing unit ~~machine~~ with privileged access to a computing resource, the method comprising the steps of:

denying the computing unit access to the computing resource for failure to provide adequate user identifying information;

obtaining credentials with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit;

providing the credentials to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource; and

establishing limited access to the computing resource using authorization information obtained from the authenticator to reflect a relative security level ~~credentials~~ for a user of the mobile computing unit, the authorization information corresponding to the authenticated identity of the mobile computing unit.

22. (Currently Amended) A computer-readable medium as in claim 21, ~~having computer executable instructions for performing the step of using the machine identity is conditional on the~~ wherein failure to provide adequate user identifying information further comprises failure of a user on the ~~machine~~ mobile computing unit to complete a log-in to gain unlimited access to the computing resource.

23. (Original) A computer-readable medium as in claim 21 having computer executable instructions wherein the mobile computing unit communicates with the computing resource using at least one wireless link.

24. (Original) A computer-readable medium as in claim 21 having computer executable instructions wherein the authorization information includes a key for encrypting communications from the mobile computing unit to an input port.

25. (Original) A computer-readable medium as in claim 21, having computer executable instructions for performing the additional step of storing the unique machine identifier on the mobile computing unit for subsequent use.

26. (Original) A computer-readable medium as in claim 21, having computer executable instructions for performing the additional step of storing the certificate on the mobile computing unit.

27. - 32. (Canceled)

33. (Currently Amended) A computer-readable medium having computer executable instructions for performing the steps of a method of providing a user secure access to a computing resource from an external site, the method comprising the steps of:

sending a request to access a computing resource;

providing a user identifier, the user identifier corresponding to an asserted identity, to initiate a log-in in order to access the computing resource;

providing, in response to a challenge, a certificate ~~credentials~~ to authenticate the asserted identity to obtain access to the computing resource; and

receiving an address for sending and receiving data to and from the computing resource based on the asserted identity.

34. (Currently Amended) A computer-readable medium as in claim 33 ~~having computer executable instructions~~ wherein the address for sending and receiving data is a universal resource locator.

35. (Original) A computer-readable medium as in claim 34 having computer executable instructions for performing the step of receiving a key for encrypting communications to the computing resource.

36. (Original) A computer-readable medium as in claim 35 having computer executable instructions for performing the step of using the key to decrypt communications from the computing resource.

REMARKS

Reconsideration and allowance in view of the foregoing amendments and the following remarks are respectfully requested. Claims 1-9, 16-19, 21-26 and 33-36 remain pending for examination.

Claim Rejections Under §103

Claims 1-9, 16, 20-26, and 33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,371,794 issued to Diffie, *et al.* (hereafter "Diffie") in view of U.S. Patent No. 5,369,702 issued to Luckenbaugh (hereafter "Luckenbaugh"). Applicant respectfully traverses this rejection.

Diffie discloses a method and apparatus for providing a secure wireless communication link between a mobile nomadic device and a base computing unit. As with many schemes, network security is provided by a base computing device providing a challenge to a mobile computing device. If the mobile computing device can respond successfully to the challenge (after performing some specified encryption operations) then the mobile computing device is allowed access to the base computing device.

It is important to note with regard to one or more of the present claims that according to Diffie, if the certificate associated with the mobile device is invalid or if a base signature of a certificate associated with the base computing device is invalid, access to the base computing device is denied. Hence, a mobile requests access to a base; the base issues a challenge to the mobile; if the mobile answers the challenge successfully the mobile is allowed to access the base; and if the mobile fails the challenge the mobile is not allowed to access the base.

Luckenbaugh discloses an object-oriented framework that facilitates development and alteration of access control systems for arbitrary applications. Arbitrary security policies are accommodated by providing for creation of labels for portions of a resource

such as an application or portions of files. Label and credential objects can be compared or correlated for granting or denying access to portions of a resource. This results in a decoupling of security policy from security enforcement and allows reconciliation of security policies having inconsistent requirements as well as development of hybrid and customized security policies.

Claim 1 has been amended and now recites a "method of providing a mobile computing unit with privileged access to a computing resource." The method includes steps of: (1) "determining that the mobile computing unit has failed to present adequate user identifying information when attempting to access the computing resource;" (2) "obtaining credentials with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit; (3) "providing the credentials to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource;" and (4) "establishing limited access to the computing resource using authorization information obtained from the authenticator that reflects a relative security level for a user of the mobile computing unit, the authorization information corresponding to the authenticated identity of the mobile computing unit."

It is noted that part of the amendment to claim 1 is the addition of element (1) listed above. This element recites that the other steps are taking upon the failure of a mobile computing unit to present adequate credentials to access a computing resource. This limitation was formerly includes in previous claims 5 and 6 but has been put in more generic terms in claim 1. Claims 5 and 6 further clarify the failure of the mobile computing unit to present adequate credentials.

Claim 1 describes a scenario in which it would be advantageous to allow a mobile computing unit to access a portion of a network resource even though it cannot be authenticated to a degree to allow it to securely access other portions of the network resource. For example, an enterprise user who is using a mobile unit may need to access an email server at the enterprise. Although a secure connection may not be established

for the mobile unit to access other secure servers in the system, a system implementing the method of claim 1 could be used to allow a secure connection to the email server while disallowing access by the mobile unit to other parts of the network.

Neither of the cited references nor a combination thereof teaches or suggests the elements recited in claim 1. Diffie specifically states that when adequate credentials cannot be presented by a mobile unit, then communication between the mobile unit and the base unit is aborted. (See Diffie, Abstract). Although Luckenbaugh teaches allowing access to different parts of a resource based on security credentials, Luckenbaugh is concerned with providing object-level solutions for ease of application. Luckenbaugh does not teach or suggest the elements recited in claim 1.

Accordingly, claim 1 is allowable over the cited reference and the rejection thereof should be withdrawn.

Claims 2-9 depend from claim 1 and are allowable at least by virtue of that dependency.

Claims 10 and 11 have been canceled, thus rendering the rejection thereof moot.

Claim 16 has been amended and recites a method of "providing a user secure access to a computing resource from an external site, the method comprising the steps of: (1) "sending a request to access a computing resource;" (2) "providing a user identifier, the user identifier corresponding to an asserted identity, to a proxy authenticating server via a remote access point;" (3) "providing, in response to a challenge, a certificate to authenticate the asserted identity, to the proxy authenticating server via the remote access point;" and (4) "receiving an address for sending and receiving data to and from the computing resource, the address corresponding to limited access to the computing resource based on the asserted identity."

In brief, claim 16 describes steps performed by a mobile device in gaining access to a secure computing resource. The mobile device receives a challenge from an authenticating server (a proxy) in response to a request from the mobile device to access

the resource. The authenticating server directs a connection to a limited portion of the resource by providing a communications address to the mobile unit. Communications directed to that particular address cannot access certain secure portions of the resource.

Neither of the cited references nor a combination thereof teaches or suggests the elements recited in claim 16. In particular, step (4) from above ("receiving an address for sending and receiving data to and from the computing resource, the address corresponding to limited access to the computing resource based on the asserted identity") is clearly distinguishable from the cited art.

Accordingly, claim 16 is allowable over the cited references and the rejection of claim 16 should be withdrawn.

Claims 17-19 depend from claim 16 and are allowable at least by virtue of that dependency. Accordingly, the rejection of these claims should also be withdrawn.

Claim 20 has been canceled, thus rendering the rejection thereof moot.

Claim 21 has been amended and now recites a "computer-readable medium having computer executable instructions for performing the steps of a method of providing a mobile computing unit with privileged access to a computing resource." The method includes steps of: (1) "denying the computing unit access to the computing resource for failure to provide adequate user identifying information;" (2) "obtaining credentials with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit;" (3) "providing the credentials to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource;" and (4) "establishing limited access to the computing resource using authorization information obtained from the authenticator to reflect a relative security level for a user of the mobile computing unit, the authorization information corresponding to the authenticated identity of the mobile computing unit.

The elements of claim 21 are similar to those recited in claim 1 and by the same rationale discussed in the response to the rejection of claim 1, above, claim 21 is

allowable over the cited references. Particularly, the notion of obtaining credentials for a mobile unit to gain limited access to a resource after it has been determined that the mobile device cannot (or has not) provided adequate credentials for extended access to the resource is not taught or suggest by the references, standing alone or taken together.

Accordingly the rejection of claim 21 should be withdrawn.

Claims 22-26 depend from claim 21 and are allowable at least by virtue of that dependency.

Claims 27 and 28 have been canceled, thus rendering the rejection thereof moot.

Claim 33 has been amended to remove an amendment made in the response to the previous office action. Claim 33 recites "a computer-readable medium having computer executable instructions for performing the steps of a method of providing a user secure access to a computing resource from an external site." The method includes steps of: (1) "sending a request to access a computing resource;" (2) "providing a user identifier, the user identifier corresponding to an asserted identity, to initiate a log-in in order to access the computing resource;" (3) "providing, in response to a challenge, a certificate to authenticate the asserted identity to obtain access to the computing resource;" and (4) "receiving an address for sending and receiving data to and from the computing resource based on the asserted identity."

Claim 33 is similar to claim 16, discussed above, in that it provides an address to a mobile device that allows the mobile device to communication with the computing resource on a limited basis. If the mobile device cannot gain full access to the computing resource, an authentication authority provides a certificate and an address to the mobile device that allows the mobile device to communicate with the computing resource on a limited basis.

Neither of the cited references, standing alone or taken together, teaches or suggests the elements recited in claim 33. Accordingly, claim 33 is allowable over the cited references and the rejection of claim 33 should be withdrawn.

Claims 34-36 depend from claim 33 and are allowable at least by virtue of that dependency. Accordingly, the rejection of these claims should also be withdrawn.

CONCLUSION

All objections and rejections having been addressed, it is respectfully submitted that the present application is now in condition for allowance. Early and forthright issuance of a Notice of Allowability is respectfully requested. If any issues remain that prevent allowance of the present application, the Examiner is urged to contact the undersigned attorney at the telephone number listed below or via the email address stated below.

Respectfully Submitted,

Microsoft Corporation

Dated: June 9, 2006

James R. Banowsky
Reg. No. 37,773
(425) 705-3539
jimban@microsoft.com

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

CERTIFICATE OF MAILING OR TRANSMISSION
(Under 37 CFR § 1.8(a)) or ELECTRONIC FILING

I hereby certify that this correspondence is being electronically deposited with the USPTO via EFS-Web on the date shown below:

June 9, 2006
Date

Signature

Noemi Tovar
Printed Name